Solution House Software (Pty) Ltd

PASSWORD POLICY

OF

SOLUTION HOUSE SOFTWARE and all its subsidiaries (Hereinafter referred to as SHS)

May 2021

Version: 1.0

1. Policy

The procedures set out in this document are governed by the Information Security Policy.

2. Scope

These procedures are applicable to:

2.1 SHS employees

2.2 Consultants

2.3 Contractors and Sub-contractors

and their respective facilities supporting SHS operations, who use it's services and assets, and where SHS data is stored or processed, including any third party contracted by SHS to handle, process, transmit, store or dispose of data, whether SHS is the data owner or is acting upon the instruction of its' customers.

3. Password/Passphrase Standards

3.1 Passwords are used for various purposes at SHS, in order to gain access to:

- The SHS backend systems
- Incident Desk application and services
- Web application accounts
- Email accounts

3.1.1 Password Composition Guidelines

a. Passwords must be a minimum of eight alphanumeric characters in length.
b. Passwords must include at least (one) 1 upper and (one) 1 (lower case character (e.g., a-z, A-Z).
c. Passwords must include punctuation marks, numeric and special characters **where this functionality is available**.

3.1.2 Password Management

a. On receipt of an initial or reset password, users must immediately change the password.
b. Passwords should never be written down and left in clear view near workstations or insecure locations.
c. Passwords should not be stored in plain text.
d. Passwords should not be shared with anyone, including executives or colleagues
e. Passwords must not be inserted into email messages or other forms of electronic communication without strong encryption.
f. Passwords believed to have been compromised, must be changed immediately and the matter referred to the Information Officer.

4. Compliance and Enforcement

4.1 Violation of this policy, will lead to restriction of access to information, and the relevant disciplinary action or penalty

4.2 Any damage, security breach or loss of information which can be deemed to have been caused by negligence or intention on the part of the user or any identified individual will be the responsibility of that user or that individual. The penalty, thereof, will be determined by the SHS disciplinary process, as above.

4.3 SHS may use any legislation relevant to the usage or protection of Information Systems (or information), in prosecuting the person who has violated this policy.

5. Policy Review

This policy shall be reviewed on at least an annual basis to

5.1 Determine if there have been changes in International, National or Internal references that may impact on this policy.

5.2 Determine if there are improvements or changes within the SHS systems or processes that should be reflected in this policy